IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

GREGGORY WILSON, individually, and on behalf of all others similarly situated, Plaintiff, v. **NAVY FEDERAL CREDIT UNION**, Defendant.	Case No.:1:22-cv-1176 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Greggory Wilson, individually and on behalf of all others similarly situated, hereby brings this Class Action Complaint against Defendant Navy Federal Credit Union ("Navy Federal," "NFCU," or "Defendant") and alleges as follows:

INTRODUCTION

1. The Zelle money transfer system is rife with fraud—fraud that places all Zelle users at an acute and immediate risk. Billions of dollars of fraudulent transactions are processed by the service each year. Victims of Zelle fraud, like Plaintiff, are often left devastated by such fraud, which can drain hundreds or thousands of dollars from their bank accounts.

2. But when Zelle fraud victims turn to NFCU for help, NFCU has a simple, repeated, bad faith response: it is your fault, you are on your own, and we will not help.

3. NFCU fails victims of Zelle fraud in two distinct ways.

4. First, NFCU maintains a massive bureaucratic apparatus designed to make it impossible for victims of Zelle fraud to lodge a successful fraud claim. When such victims make a claim for fraud, and as occurred to Plaintiff, NFCU denies the claim without conducting a full investigation and blames fraud victims for the fraud. As occurred with Plaintiff, NFCU summarily rejected fraud claims without explanation or recourse.

5. Second, NFCU violates plain promises in its contract documents that its' accountholders will be protected in the event of fraudulent Zelle transfers.

6. NFCU's policies and practices also violate the Electronic Fund Transfer Act ("EFTA") a statute with the purpose of "provid[ing] a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund and remittance transfer systems." *Id.* § 1693(b). "The primary objective of [the EFTA] is the provision of individual consumer rights." *Id.*

7. This lawsuit is brought as a class action on behalf of Plaintiff and similarly situated customers of Navy Federal who: have been the victim of fraud on the Zelle service; who have incurred losses due to that fraud that have not been reimbursed by NFCU; and who were entitled by NFCU's contract promises and EFTA to a full reimbursement of losses caused by fraud on the Zelle service.

8. Plaintiff seeks actual damages, punitive damages, restitution, and an injunction on behalf of the general public to prevent Navy Federal from continuing to engage in its illegal practices as described herein.

PARTIES

9. Plaintiff Greggory Wilson is a citizen and resident of Cleveland, Tennessee.

10. Defendant Navy Federal Credit Union is a national credit union with its principal place of business in Vienna, Virginia.

JURISDICTION AND VENUE

11. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332(d)(2), because the matter in controversy exceeds $5,000,000, exclusive of interest and costs, and is a class action in which at least one member of the class is a citizen of a different State than Defendant. The number of members of the proposed Classes in aggregate exceeds 100 users. 28 U.S.C. § 1332(d)(5)(B).

12. This Court has personal jurisdiction over the Defendant because it regularly conducts and/or solicits business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from products and/or services provided to persons in this District.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this District and because a substantial part of the events or omissions giving rise to the claims occurred in this District.

FACTUAL ALLEGATIONS

A. Zelle – The Favorite App of Fraudsters

14. Created in 2017 by America's largest banks[1] to enable digital money transfers, Zelle comes embedded in banking apps and is now America's most widely used money transfer service, outpacing its closest rival (Venmo) by $260 billion in transfers in 2021.[2]

15. About 1.8 billion payments—totaling $490 billion—were sent by consumers and businesses through the Zelle Network in 2021, according to the Early Warning Services. Total dollars transferred were up 59% from 2020.[3]

16. Nearly 18 million people have been victims of "widespread fraud" on money transfer apps, according to a letter sent in late April of 2022 to Zelle by U.S. Senators Elizabeth Warren of Massachusetts, Robert Menendez of New Jersey and Jack Reed of Rhode Island.[4]

---

[1] Bank of America, Capital One, JPMorgan Chase, PNC, BB&T (now Truist), U.S. Bank and Wells Fargo.

[2] Cowley, Stacy & Nguyen, Lananh, "Fraud is Flourishing on Zelle. The Banks Say It Is Not Their Problem," *New York Times* (March 6, 2022), https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html (last visited September 13, 2022).

[3] ZellePay.com, *Nearly Half a Trillion Dollars Sent by Consumers and Businesses with Zelle in 2021* (February 02, 2022), https://www.zellepay.com/press-releases/nearly-half-trillion-dollars-sent-consumers-and-businesses-zelle-2021 (last visited September 21, 2022).

[4] Letter from Elizabeth Warren, Robert Menendez, Jack Reed, Sen., U.S. Cong., to Al Ko, CEO, Early Warning Services (April 2, 2022).

17. "Zelle's biggest draw—the immediacy of its transfers—also makes scams more effective and 'a favorite of fraudsters,' as consumers have no option to cancel a transaction even moments after authorizing it," the letter stated.

18. The 1,500 banks and credit unions who are members of the Zelle network, including Navy Federal, know full well that they have a widespread fraud problem on their hands, but have failed to protect their accountholders who fall prey to fraud.

19. In short, and unbeknownst to average Navy Federal customers, the Zelle network has become a preferred tool for fraudsters like romance scammers, cryptocurrency con artists, landlord impersonators, and those who use social media sites to advertise fake concert tickets, used cars, and purebred puppies—or, as in Plaintiff's case, simply for those who steal phones, computers, and user data and then use their access to drain money from accounts via Zelle.

20. As one U.S. Senator said to CEOs of some of the banks that own Zelle: "Zelle is not safe. You built the system, you profit from every transaction on the system and you tell people that it is safe. But when someone is defrauded, you claim that's the customer's problem," said Senator Elizabeth Warren, during a Senate Banking Committee hearing in September 2023.

21. Worse, even consumers who disputed "*unauthorized"* Zelle transfers and who were not duped by fraudsters to initiate the Zelle transfer, such as Plaintiff, are not being reimbursed and protected by their banks, according to an October 2022 Senate report about fraud on Zelle. Data from Bank of America, U.S. Bank, PNC Bank and Truist revealed that they reimbursed consumers for only 47% of the dollar amount of cases in which customers reported unauthorized payments on Zelle in 2021 and the first half of 2022.[5]

[5] "Facilitating Fraud: How Consumers Defrauded on Zelle are Left High and Dry by the Banks that Created It," Office of Sen. Elizabeth Warren,

22. Navy Federal claims to have a "zero liability policy" for cases in which a bad actor gains access to a consumer's account and uses it to make unauthorized Zelle transfers, but it fails to keep this promise.

23. On information and belief, NFCU uses Zelle to insulate itself from financial liability for fraudulent and unauthorized transactions.

B. Navy Federal Fails to Follow Regulatory Guidance

24. Recent CFPB guidance on Electronic Fund Transfers ("EFTs") indicates person-to-person ("P2P") payments are EFTs, such as transactions made with Zelle, and trigger "error resolution obligations" to consumers to protect them from situations that results in unauthorized EFTs from their accounts. [6]

25. An unauthorized EFT is an EFT from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. 12 CFR 1005.2(m). Unauthorized EFTs include transfers initiated by a person who obtained a consumer's access device or account access information through fraud or robbery and consumer transfers at an ATM that were induced by force. Comments 2(m)-3 and 4.

26. Other examples of situations involving unauthorized EFTs includes, according to the CFPB, when a thief steals a consumer's debit card and initiates a payment using the consumer's stolen debit card; when a fraudster uses a bank-provided P2P payment application to initiate a

---

https://www.warren.senate.gov/imo/media/doc/ZELLE%20REPORT%20OCTOBER%202022.pdf (last visited October 10, 2022).

[6] "Electronic Fund Transfers FAQs," Consumer Financial Protection Bureau, https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accountsresources/electronic-fund-transfers/electronic-fund-transfers-faqs/#financial-institutions-2 (last visited June 28, 2022).

credit push payment out of the consumer's deposit account; and/or when a fraudster hacks into a consumer's phone and uses the mobile wallet to initiate a debit card transfer out of the consumer's account.[7]

27. Additionally, the Federal Deposit Insurance Corporation ("FDIC") issued a report in March 2022 finding that Regulation E's "liability protections for unauthorized transfers apply even if a consumer is deceived into giving someone their authorization credentials."[8] Further, the FDIC stated that "[c]onsumer account disclosures cannot limit protections provided for in the regulation."[9] The FDIC stated that both the banks and Money Payment Platforms ("MPPs"), such as Zelle, are considered "financial institutions" under Regulation E, and as such have investigative and error resolution obligations under Regulation E.

28. On information and belief, Navy Federal does not reimburse consumers for losses from unauthorized EFTs due to Zelle fraud, even where the losses are timely reported by consumers.

C. Navy Federal Breaches Contract Promises and the Implied Covenant and Misrepresents Fraud Protections Regarding Zelle in its Account Contracts

29. Navy Federal's Deposit Agreement (the "Deposit Agreement"), attached as **Exhibit 1**, applicable to consumer accounts repeatedly promises users that, if they timely report fraud, such fraud will be fairly investigated and accountholders will not be liable for fraudulent transfers.

---

[7] *Id.*
[8] FDIC, *Consumer Compliance Supervisory Highlights Federal Deposit Insurance Corporation* (March 2022), https://www.fdic.gov/regulations/examinations/consumer-compliance-supervisory-highlights/documents/ccs-highlights-march2022.pdf (last accessed Sept. 21, 2022).
[9] *Id.*

30. Zelle is never mentioned by name, not even a single time, in the Deposit Agreement that accountholders receive when opening a Navy Federal account.

31. With respect to transactions governed by Regulation E, the Agreement provides:

> **Your Liability for Unauthorized Electronic Funds Transfers**
> **Notify us AT ONCE if you believe:**
> - your account may have been accessed without your authority;
> - your card, code, or password has been lost or stolen;
> - someone has transferred or may transfer money from your account without your permission; or
> - an electronic funds transfer has been made without your permission using information from your check or your MMSA check
>
> The best way to minimize your possible loss is to telephone or, if you have Online Banking, contact us through our eMessaging system at **navyfederal.org**, although you may advise us in person or in writing. See the telephone numbers and address listed at the end of this agreement and disclosure. If you do not notify us, you could lose all the money in your account (*plus your maximum line of credit amount*).
>
> If you tell us within two (2) business days after you discover your password or other means to access your account has been lost or stolen, your liability is no more than $50.00 should someone access your account without your permission. If you do not tell us within two (2) business days after you discover such loss or theft, and we can prove that we could have prevented the unauthorized use of your password or other means to access your account if you had told us, you could be liable for as much as $500.00.
>
> **Also, if your statement shows transfers that you did not make or authorize, tell us AT ONCE**. If you do not tell us within sixty (60) days after the statement was delivered to you of any unauthorized or fraudulent use of your account, you may not get back any of the money you lost after the sixty (60) days if we can prove that we could have stopped someone from taking the money if you had told us in time. If a good reason (such as a long trip or a hospital stay) prevented you from telling us, we may in our sole discretion extend the time periods.
>
> **In Case of Errors or Questions about your Electronic Transfers**
> If you think your statement or receipt is wrong, or if you need more information about a transaction listed on your statement or receipt, contact us as soon as possible at the telephone numbers and address listed at the end of this agreement and disclosure.
>
> We must hear from you no later than sixty (60) days after the FIRST statement on which the problem or error appeared… We will determine whether an error occurred within ten (10) business days (*twenty (20) business days for new accounts*)

> after you notify us of the error and will correct any error promptly… If it is determined that there was no error, we will… send you a written explanation within three (3) business days… You may ask for copies of documents used in our investigation.

See Deposit Agreement, at 11-12.

32. These provisions are and were reasonably understood by Plaintiff to mean that Plaintiff would not be liable for electronic funds transfers effectuated by fraud.

33. Indeed, Navy Federal's Zelle Terms and Condition (the "Zelle Terms"), attached as **Exhibit 2**, also indicates that accountholders will not be liable for fraudulent transactions, if reported timely.

34. The Zelle Terms state:

> **9. Liability for Unauthorized Transfers**
>
> **NOTIFY NAVY FEDERAL AT ONCE if you believe:**
> - **your account has been accessed without your authorization;**
> - **your debit card, username, or password has been lost, stolen, compromised, or used or can be used without your authorization;**
> - **someone has transferred or can transfer money from your account without your permission; or**
> - **your statement shows transfers out of your account that you did not make or authorize.**
>
> The best way to minimize your possible losses is to take steps to secure the compromise, for example, freeze your debit card and change your username and password, and contact Navy Federal as soon as possible using the contact information in Section 17.
>
> If you do not notify us, you could lose all the money in your account (plus your maximum Checking Protection amount if you enrolled). If the unauthorized Zelle payment was made via ACH, see the Important Important Disclosures (NFCU 606) for more information on your potential liability. If the unauthorized Zelle payment was made via debit card, see the Debit Card Disclosure (NFCU 210AB), which includes Navy Federal's Zero Liability policy, for more information on your potential liability.
>
> **10. Error Resolution**
> If you think your account statement or transaction history has errors, or if you need more information about a transaction listed on your account statement or transaction history, contact Navy Federal as soon as possible using the contact information in Section 17. You MUST notify us of suspected errors no later than sixty (60) days after we FIRST make

> available your account statement on which the suspected error appeared. You will need to identify yourself and your account, describe the error or the transaction you are questioning, clearly explain why you believe an error exists or why you need more information, and tell us the dollar amount of the suspected error.

See Zelle Terms, at 13.

35. The Zelle Terms also promises that Navy Federal will take active steps to detect and prevent fraud, which it failed to do: "the [Zelle] transfer may be blocked to prevent fraud or comply with regulatory requirements. If we delay or block a payment that you have initiated, we will notify you by email or text message and may request you or the recipient to take additional action." *Id.*, at 10.

36. The Zelle Terms refers to and incorporates yet another agreement, the Debit Card Disclosure, attached as **Exhibit 3**.

37. The Debit Card Disclosure contains a simple, straightforward "Zero Liability" promise: "Navy Federal's Zero Liability Policy for Fraud: [I]f you notify us of suspected fraud within 60 days of the statement date on which the fraudulent transactions first appear, ***we will not hold you responsible for confirmed fraudulent transactions***." Debit Card Disclosure at para. 15 (emphasis added)

38. These provisions are and were reasonably understood by Plaintiff to mean that Plaintiff would not be liable for Zelle transfers effectuated by fraud.

39. As alleged with specificity herein, Navy Federal breached the Deposit Agreement, the Zelle Terms, and the Debit Card Disclosure (collectively, the "Agreements"). Navy Federal adopted an unreasonable and unfair understanding of the Agreements' term "unauthorized."

40. The term "unauthorized" reasonably encompasses all transactions occurring as a result of fraud. In other words, no fraudulent or fraud-induced transition can reasonably be considered "authorized."

41. NFCU unfairly and improperly considers fraudulent Zelle transactions to be "authorized," thus shirking fraud protection promises it otherwise makes in the Agreements.

42. Moreover, and with respect to consumers like Plaintiff, whose account was compromised by a third party without permission and then used by the fraudster for fraudulent transactions, NFCU has adopted an investigation practice that almost always rejects valid claims, in breach of the implied covenant.

D. Plaintiff Wilson's Experience

43. On June 30, 2019, Plaintiff Wilson discovered a series of Zelle transfers from his Navy Federal account that he never authorized. In total, there were seven (7) unauthorized Zelle transfers that spanned from January 2019 to April 2019 amounting to $4,630.

44. Plaintiff Wilson did not, and does not, know the identity of the recipients.

45. Plaintiff Wilson never downloaded and signed up for Zelle.

46. The next day, on July 1, 2019, Plaintiff Wilson reported the unauthorized Zelle transactions to Navy Federal's fraud department and also to the Federal Bureau of Investigation.

47. Navy Federal's fraud department provided its theory as to how the fraud happened: In 2018, Plaintiff Wilson requested a new checking account number and closed his then-current checking account because it had been compromised. Navy Federal, however, failed to assign a new debit card and left Plaintiff's prior debit card linked to the new checking account. Therefore, Navy Federal believed that fraudsters likely had his prior debit card information and used it to make the Zelle transfers. Navy Federal further stated that it should have assigned a new debit card at the time the new checking account was opened.

48. Navy Federal advised Plaintiff Wilson that it was cancelling his prior, old debit card and also requested Plaintiff submit a written statement of the fraud.

49. Following the instruction of Navy Federal's fraud department, Plaintiff Wilson mailed Navy Federal a written statement with specific details of the unauthorized Zelle transactions such as date, amount, and recipients.

50. On three separate occasions, Plaintiff Wilson contacted Navy Federal by phone to follow up on his claim. Each time Plaintiff was advised to submit fraud paperwork or encouraged to contact Zelle. Plaintiff Wilson complied with all of Navy Federal's instructions, including contacting Zelle.

51. Despite Plaintiff Wilson's detailed dispute, NFCU denied his claim as it determined there was "no error" and refused to reimburse him for his loss.

52. On July 25, 2019, Navy Federal sent a letter to Plaintiff Wilson stating that: "Based on a thorough investigation of your account activity, we have determined that no error has occurred. The provisional credit of $4630.00 applied to your checking account on 07/15/19 will be reversed on 7/25/19."

53. Even though Plaintiff did not authorize any such transfer of funds from his Navy Federal account, Navy Federal would still not approve his claim and failed to provide any details of the investigation or provide a rationale for their decision other than determining "no error has occurred."

54. Since Navy Federal improperly denied Plaintiff's claim, he submitted a complaint to the Consumer Financial Protection Bureau on August 27, 2019. In response, Navy Federal maintained that it "conducted an investigation and determined that there was no unauthorized activity."

55. Like other customers that have had their accounts debited (and in some cases drained) by imposters and scam artists, NFCU denied Plaintiff Wilson's claim seeking reversal of

the unauthorized transactions stating that these victims had authorized payments and were responsible for the loss.

CLASS ALLEGATIONS

56. Plaintiff brings this action individually and as representatives of all those similarly situated, on behalf of the below-defined Classes:

> **Nationwide Class:**
> All persons with a Navy Federal account who reported Zelle transfer(s) they did not authorize to Defendant and incurred unreimbursed losses.
>
> **Tennessee Class:**
> All Tennessee persons with a Navy Federal account who reported Zelle transfer(s) they did not authorize to Defendant and incurred unreimbursed losses.

57. Excluded from the Classes are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staffs.

58. This case is appropriate for class treatment because Plaintiff can prove the elements of their claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

59. **Numerosity:** The members of the Classes are so numerous that joinder of all members would be unfeasible and impracticable. The precise membership of the Classes are unknown to Plaintiff at this time; however, it is estimated that the Classes number is greater than one hundred individuals. The identity of such membership is readily ascertainable via inspection of Defendant's books and records or other approved methods. Class members may be notified of the pendency of this action by mail, email, internet postings, and/or publication.

60. **Common Questions of Law or Fact:** There are common questions of law and fact as to Plaintiff and all other similarly situated persons, which predominate over questions affecting only individual Class members, including, without limitation:

a) Whether Plaintiff and the Class members were damaged by Defendant's conduct;

b) Whether Defendant's actions or inactions breached its contractual promises;

c) Whether Defendant's actions or inactions violated the EFTA; and

d) Whether Plaintiff and the Class are entitled to a preliminary and permanent injunction enjoining Defendant's conduct.

61. **Predominance of Common Questions:** Common questions of law and fact predominate over questions that affect only individual members of the Classes. The common questions of law set forth above are numerous and substantial and stem from Defendant's uniform practices applicable to each individual Class member. As such, these common questions predominate over individual questions concerning each Class member's showing as to his or her eligibility for recovery or as to the amount of his or her damages.

62. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the Classes because, among other things, Plaintiff and all Class members were similarly injured through Defendant's uniform misconduct as alleged above. As alleged herein, Plaintiff, like the members of the Classes, were deprived of monies that rightfully belonged to them. Further, there are no defenses available to Defendant that are unique to Plaintiff.

63. **Adequacy of Representation:** Plaintiff is an adequate class representative because he is fully prepared to take all necessary steps to represent fairly and adequately the interests of the members of the Classes, and because their interests do not conflict with the interests of the other Class members they seek to represent. Moreover, Plaintiff's attorneys are ready, willing, and

able to fully and adequately represent Plaintiff and the members of the Class. Plaintiff's attorneys are experienced in complex class action litigation, and they will prosecute this action vigorously.

64. **Superiority:** The nature of this action and the claims available to Plaintiff and members of the Classes make the class action format a particularly efficient and appropriate procedure to redress the violations alleged herein. If each Class member were required to file an individual lawsuit, Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Plaintiff with its vastly superior financial and legal resources. Moreover, the prosecution of separate actions by individual Class members, even if possible, would create a substantial risk of inconsistent or varying verdicts or adjudications with respect to the individual Class members against Defendant, and which would establish potentially incompatible standards of conduct for Defendant and/or legal determinations with respect to individual Class members which would, as a practical matter, be dispositive of the interests of the other Class members not parties to adjudications or which would substantially impair or impede the ability of the Class members to protect their interests. Further, the claims of the individual members of the Classes are not sufficiently large to warrant vigorous individual prosecution considering all of the concomitant costs and expenses attending thereto.

FIRST CAUSE OF ACTION
Breach of Contract Including Breach of the Covenant of Good Faith and Fair Dealing
(Asserted on Behalf of the Classes)

65. Plaintiff repeats and realleges the above allegations as if fully set forth herein.

66. Plaintiff and Members of the Classes contracted with Navy Federal for checking account services, as embodied in the Deposit Agreement.

67. Navy Federal breached the terms of its contract with consumers when as described herein, Navy Federal failed to reimburse fraudulent or unauthorized transactions on the Zelle

money transfer service and failed to reimburse accountholders for fraudulent losses incurred using the Zelle service.

68. Further, under the law of each state where Defendant conducts business, an implied covenant of good faith and fair dealing govern every contract. For banking transactions, this is also mandated by the Uniform Commercial Code that has been adopted in each state. The covenant of good faith and fair dealing constrains Defendant's discretion to abuse self-granted contractual powers.

69. This good faith requirement extends to the manner in which a party employs discretion conferred by a contract.

70. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form. Evading the spirit of the bargain and abusing the power to specify terms constitute examples of bad faith in the performance of contracts.

71. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes his conduct to be justified. A lack of good faith may be overt or may consist of inaction, and fair dealing may require more than honesty. Other examples of violations of good faith and fair dealing are willful rendering of imperfect performance, abuse of a power to specify terms, and interference with or failure to cooperate in the other party's performance.

72. Defendant breached the covenant of good faith and fair dealing when it failed to fairly investigate reported fraudulent transactions on the Zelle money transfer service, failed to

reimburse accountholders for fraudulent losses incurred using the Zelle service, and adopted an unfair and unreasonable definition of the term "unauthorized transaction."

73. Each of Defendant's actions was done in bad faith and was arbitrary and capricious.

74. Plaintiff and Members of the Classes have performed all, or substantially all, of the obligations imposed on them pursuant to the Deposit Agreement.

75. Plaintiff and Members of the Classes have sustained monetary damages as a result of each of Defendant's breaches of the Deposit Agreement and covenant of good faith and fair dealing.

SECOND CAUSE OF ACTION
Unjust Enrichment
(Asserted on Behalf of the Classes)

76. Plaintiff repeats and realleges the above allegations as if fully set forth herein, in the alternative to the breach of contract cause of action:

77. Defendant has been conferred the benefit or enrichment by keeping funds that they are otherwise obligated to replace for Plaintiff and Members of the Classes pursuant to Regulation E's error resolution obligations.

78. Defendant knew and appreciated this benefit or enrichment and the detriment or impoverishment to Plaintiff and Members of the Classes.

79. It is inequitable for Defendant to retain the benefit or enrichment of keeping these funds when it knows that, as a financial institution, it is obligated to comply with Regulation E and credit Plaintiff and Members of the Classes' accounts for the amounts taken.

80. Plaintiff and Members of the Classes have sustained a detriment or an impoverishment from Defendant's failure to remedy this inequity and are entitled to restitution for the unjust enrichment to Defendant.

81. Plaintiff and Members of the Classes are entitled to restitution and disgorgement of the funds unjustly retained by Defendant in the absence of any legal relief.

THIRD CAUSE OF ACTION
Violation of the Electronic Fund Transfer Act ("EFTA")
(Asserted on Behalf of the Classes)

82. Plaintiff repeats and realleges the above allegations as if fully set forth herein.

83. The Electronic Fund Transfer Act and Regulation E apply to electronic fund transfers that authorize a financial institution to debit or credit a consumer's account. 12 C.F.R. § 1005.3(a).

84. The primary objective of the EFTA is "the protection of individual consumers engaging in electronic fund transfers and remittance transfers." 12 C.F.R. § 1005.1(b).

85. Defendant is a financial institution. 12 C.F.R. § 1005.2(i).

86. "If a financial institution, within sixty days after having transmitted to a consumer pursuant to [15 U.S.C. § 1693d(a), (c), or (d)] or notification pursuant to [15 U.S.C. § 1693d(d)] receives oral or written notice in which the consumer[:] (1) sets forth or otherwise enables the financial institution to identify the name and the account number of the consumer; (2) indicates the consumer's belief that the documentation, or, in the case of notification pursuant to [15 U.S.C. § 1693d(b)], the consumer's account, contains an error and the amount of such error; and (3) sets forth the reasons for the consumer's belief (where applicable) that an error has occurred," the financial institution is required to investigate the alleged error. 15 U.S.C. § 1693f(a).

87. After said investigation, the financial institution must determine whether an "error" has occurred and report or mail the results of such investigation and determination to the consumer within ten (10) business days. 15 U.S.C. § 1693f(a).

88. A financial institution that provisionally recredits the consumer's account for the amount alleged to be in error pending an investigation, however, is afforded forty-five (45) business days after receipt of notice of error to investigate. *Id.* § 16993f(c).

89. Pursuant to the EFTA, an error includes "an unauthorized electronic fund transfer." *Id*. § 1693f(f).

90. An Electronic Fund Transfer ("EFT") is any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account. 12 C.F.R. 1005.3(b)(1). Accordingly, Regulation E applies to any person-to-person ("P2P") or mobile payment transactions that meet the definition of EFT. 12 C.F.R. § 1005.3(b)(1)(v); *id*., Comment 3(b)(1)-1.ii.

91. Unauthorized EFTs are EFTs from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. 12 C.F.R. § 1005.2(m).

92. According to the Consumer Financial Protection Bureau, when a third party fraudulently induces a consumer into sharing account access information that is used to initiate an EFT from the consumer's account, that transfer meets Regulation E's definition of an unauthorized EFT.[10]

93. In particular, Comment 1005.2(m)-3 of Regulation E explains that an unauthorized EFT includes a transfer initiated by a person who obtained the access device from the consumer through robbery or fraud. As such, when a consumer's account access information is fraudulently obtained by a third party, and a third party uses that information to make an EFT from the consumer's account, the transfer is an unauthorized EFT under regulation E. 12 C.F.R. § 1005.2(m), Comment 1005.2(m)-3.

94. Here, third-party fraudsters made unauthorized money transfers from the Navy Federal accounts of Plaintiff and Members of the Classes.

---

[10] "Electronic Fund Transfers FAQs," Consumer Financial Protection Bureau, https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/#financial-institutions-2 (last accessed September 6, 2022).

95. After the unauthorized EFTs were made, the EFTs appeared on the bank statements of Plaintiff and Members of the Classes.

96. Plaintiff and Members of the Classes notified Defendant of these errors within sixty (60) days of their appearances on their accounts.

97. As a direct and proximate result of Defendant's conduct, Plaintiff and Members of the Classes were unable to reclaim the account funds taken from scammers from unauthorized EFTs.

98. Defendant knowingly and willfully concluded that the transfers of funds via Zelle on accounts of Plaintiff and Members of the Classes were not in error when such conclusions could not reasonably have been drawn from the evidence available to the financial institutions at the time of the investigation. 15 U.S.C. § 1693f(e)(2).

99. Defendant intentionally determined that the unauthorized transfer of funds via Zelle on accounts of Plaintiff and Members of the Classes were not in error due to, at least in part, its financial self-interest.

100. Defendant refused to reverse or refund funds to Plaintiff and Members of the Classes.

101. As such, Plaintiff and Members of the Classes are each entitled to (i) actual damages; (ii) treble damages; (iii) the lesser of $500,000.00 or one percent (1%) of the net worth of Defendant; and (iv) reasonable attorneys' fees and costs. *Id*. §§ 1693f(e)(2), 1693m(a)(2)(B)–(3).

FOURTH CAUSE OF ACTION
NEGLIGENCE
(Asserted on Behalf of the Classes)

102. Plaintiff repeats and realleges the above allegations as if fully set forth herein.

103. Defendant owed Plaintiff and Members of the Classes at least a duty to take reasonable steps to safeguard their financial information and protect their financial accounts from malicious third parties, to adequately warn of known risks and/or dangers associated with the Zelle

mobile application, and to properly investigate disputed transactions initiated and consummated through the Navy Federal and/or Zelle app.

104. Defendant breached its obligations to Plaintiff and Members of the Classes and as otherwise negligent and/or reckless by at least:

(a) Failing to maintain an adequate data security measures to prevent or reduce the risk of disclosure of the names, phone numbers, and bank affiliation of Plaintiff and Members of the Classes to malicious third parties;

(b) Failing to adequately protect the private information of Plaintiff and Members of the Classes;

(c) Failing to properly warn Plaintiff and Members of the Classes of the risks and/or dangers associated with the Zelle service or informing consumers about the Zelle-related scams;

(d) Failing to adequately investigate and document findings from the investigations of fraud-related EFTA disputes of the unauthorized transactions made on the accounts of Plaintiff and Members of the Classes using the Zelle payment platform;

(e) Failing to take appropriate steps to avoid unauthorized transactions through the Navy Federal Zelle mobile application in response to known scams and continuing with business as normal;

(f) Failing to implement appropriate and sufficient safeguards against scams of the nature alleged in the Complaint light of the knowledge that those scams have been rampant across the country;

(g) Failing to review account agreements and disclosures to ensure they do not attempt to diminish or limit consumers' rights under Regulation E;

(h) Permitting scammers to use Zelle's payment platform to siphon funds from the accounts of Plaintiff and the Members of the Classes;

(i) Failing to reverse unauthorized transactions pursuant to Regulation E error resolution requirements following disputes of Plaintiff and Members of the Classes despite Defendant's knowledge that said transactions were unauthorized as part of a scam that is well-known to Defendant; and

(j) Failing to permanently reverse unauthorized transactions upon a sufficient showing by Plaintiff and Members of the Classes that said transactions were unauthorized.

105. As a direct and proximate result of Navy Federal's breach, Plaintiff and Members of the Classes lost funds from their Navy Federal bank accounts.

106. Plaintiff and Members of the Classes are entitled to damages for their continuing and increased risk of fraud and their loss of money.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Classes, demands a jury trial on all claims so triable and judgment as follows:

A. Certifying the proposed Classes, appointing Plaintiff as representative of the Classes, and appointing counsel for Plaintiff as lead counsel for the respective Classes;

B. Declaring that Defendant's policies and practices as described herein constitute a breach of contract and/or breach of the covenant of good faith and fair dealing or unjust enrichment, , a violation of the Electronic Fund Transfer Act, and/or negligence.

C. Enjoining Defendant from the wrongful conduct as described herein;

D. Awarding restitution to Plaintiff and the Classes for unjust enrichment as a result of the wrongs alleged herein in an amount to be determined at trial;

E. Compelling disgorgement of the ill-gotten gains derived by Defendant from its misconduct;

F. Awarding actual and/or compensatory damages in an amount according to proof;

G. Punitive and exemplary damages;

H. Awarding pre-judgment interest at the maximum rate permitted by applicable law;

I. Reimbursing all costs, expenses, and disbursements accrued by Plaintiff in connection with this action, including reasonable attorneys' fees, costs, and expenses, pursuant to applicable law and any other basis; and

J. Awarding such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff and all others similarly situated hereby demand trial by jury on all issues in this Class Action Complaint that are so triable.

Dated: October 18, 2022

Respectfully Submitted,

/s/ Heather Whitaker Goldstein
Heather Whitaker Goldstein
Virginia State Bar No. 41480
David M. Wilkerson*
THE VAN WINKLE LAW FIRM
11 N. Market Street
Asheville, North Carolina 28801
(828)258-2991 (phone)
(828)257-2767 (fax)
hgoldstein@vwlawfirm.com
dwilkerson@vwlawfirm.com

Andrew J. Shamis*
Edwin E. Elliott*
SHAMIS & GENTILE, P.A.
14 NE First Avenue, Suite 705
Miami, Florida 33132
Telephone: 305-479-2299
ashamis@shamisgentile.com
edwine@shamisgentile.com

Jeffrey D. Kaliel*
Sophia Goren Gold*
KALIELGOLD PLLC
1100 15th Street NW, 4th Floor
Washington, D.C. 20005
Telephone: (202) 350-4783
jkaliel@kalielpllc.com
sgold@kalielgold.com

Scott Edelsberg*
Christopher Gold*
EDELSBERG LAW, PA
20900 NE 30th Ave, Suite 417
Aventura, Florida 33180
Telephone: 305-975-3320
scott@edelsberglaw.com
chris@edelsberglaw.com

**Pro Hac Vice forthcoming*

Counsel for Plaintiff and the Proposed Class